Working Group G Outbrief

25th Ground System Architectures Workshop

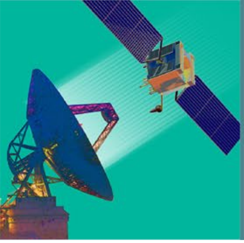
Adapting Critical Operations

Starts March 1, 2021 | Special Online Series of Events

Ontologies for Space and Ground System Cybersecurity

Leads:
John L. Crassidis
and Barry Smith,
University at Buffalo

March 11, 2021

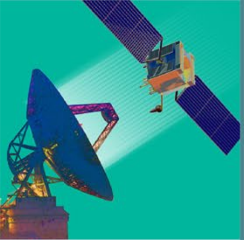


Session Goals

Ontologies for Space and Ground System Cybersecurity

- Discuss strategies to mitigate space cyberattacks, i.e. cyber-resilient satellites
- Introduce space ontologies
  - *General introduction*
  - *The Space Domain Ontologies*
    - Outer Space Ontology
    - Space Event Ontology
    - Space Object Ontology
    - Spacecraft Ontology
    - Spacecraft Mission Ontology
- Discuss how ontologies are used in space situational awareness across four segments: space, ground, link, and user
  - *Vulnerability/threat identification*
  - *Anomaly identification*
- Introduce the notion of "physics-based" cybersecurity
  - *Discuss the role of space ontologies within this approach*

Working Group G

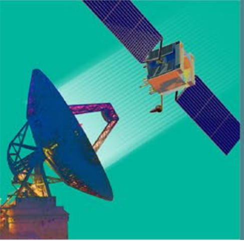


Presenters/Panelists

Ontologies for Space and Ground System Cybersecurity

- John L. Crassidis
  - *University at Buffalo, State University of New York (SUNY), SUNY Distinguished Professor, Samuel P. Capen Chair Professor*
  - *Email: johnc@buffalo.edu*
- Barry Smith
  - *University at Buffalo, SUNY, SUNY Distinguished Professor, Julian Park Chair*
  - *Email: phismith@buffalo.edu*
- Ron Rudnicki
  - *Information Fusion Group, CUBRC*
  - *Email: rudnicki@cubrc.org*
- Alexander Cox
  - *Information Fusion Group, CUBRC*
  - *Email: alexander.cox@cubrc.org*
- Mark Jensen
  - *Information Fusion Group, CUBRC*
  - *Email: mark.jensen@cubrc.org*

Working Group G

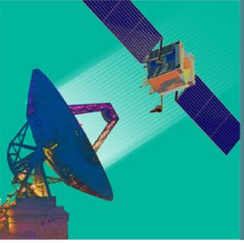


Key Points

Ontologies for Space and Ground System Cybersecurity

- Cyber threats identified by the National Air and Space Intelligence Center (NASIC)
  - *They span four segments: space, ground, link, and user*
- Effective technologies for supporting protection of U.S. space assets are required
  - *Must provide for clear and effective dissemination of complex information to end users*
- Ontologies can provide precise definitions of the terms and relations used in the space domain
  - *Necessary to ensure consistency and interoperability across the complexity of systems for space cyber defense and threat mitigation*
- Need to be proactive rather than reactive
  - *Reactive will be too late, especially for on-orbit satellites*
- Must focus equally on identification and mitigation of all space cyber threats and on related space cyber strategies
  - *Must take human subject-matter-expertise and automate it for decision making*
  - *The Space Domain Ontologies will be a vital aspect of the aforementioned strategies*

Working Group G



Conclusions

Ontologies for Space and Ground System Cybersecurity

- Must focus on all possible space cyber threats, which includes security of space assets from cyber intrusions
  - *For example, hijacking, space cyber threats such as jamming and obfuscation of satellite operations*
    - May be physical (such as blocking a satellite's view) or electronic (spoofing, use of directed-energy weapons), satellite-to-satellite communication disruptions such as relay interruptions
  - *Ground station defense*
    - Including protecting existing ground stations and mitigating adversarial ground stations meant to breach existing security systems
- Cohesive space cybersecurity ontology allows:
  - *Members of the space cybersecurity community across the globe to efficiently communicate on the basis of a shared understanding of terms, and*
  - *A common basis for exchange and analysis of data*
- Standards for space ontologies
  - *Current work is more focused on research and development*
  - *Several years before they will be standardized*

Working Group G